

УДК 004.052.42

МАРКОВСКИЙ А.П.,
САИДРЕЗА МАХМАЛИ,
ТУРЧЕНКО Ю.А.,
САКУН В.Н.

ИСПОЛЬЗОВАНИЕ ВЗВЕШЕННЫХ КОНТРОЛЬНЫХ СУММ ДЛЯ ИСПРАВЛЕНИЯ “ПАЧЕК” ОШИБОК ПЕРЕДАЧИ ДАННЫХ

Статья посвящена решению проблемы повышения эффективности обнаружения и исправления “пачек” ошибок передачи данных, вызванных внешними помехами. Для исправления “пачек” ошибок предложено использовать специальную модификацию взвешенной контрольной суммы. Разработан алгоритм обнаружения и коррекции “пачек” ошибок. Показано, что предложенная технология обеспечивает большую эффективность обнаружения и исправления ошибок по сравнению с известными корректирующими кодами.

Paper is dedicated to solving the problem of increasing the efficiency of detecting and correcting the data transmission burst errors brought on by external noises. For burst errors coorrection the utilization of special weighed check sum modification has been proposed. Algorithm for burst error detection and correction has been worked out. It has been shown that proposed techniques ensure superior data transformation error detecting and correcting effectiveness in compare to known correcting code.

Введение

К началу XXI-го века информационная интеграция стала одним из наиболее весомых факторов развития человеческой цивилизации. В свою очередь, процесс расширения информационной интеграции базируется на совершенствовании средств и технологии передачи цифровых данных. Ныне основными направлениями такого совершенствования являются повышение скорости передачи и расширение использования беспроводных каналов.

Важнейшим фактором совершенствования технологии передачи данных является обеспечение высокого уровня надежности. Это достигается как за счет повышения собственнo передачи в канале, так и за счет совершенствования специальных средств обнаружения и коррекции ошибок, возникающих при передаче данных. Поступательное развитие техники передачи данных постоянно ставит новые требования к средствам обнаружения и коррекции ошибок передачи. Так, повышение скорости передачи данных ужесточает требования к быстродействию средств контроля ошибок. Расширение использования беспроводных систем передачи данных имеет следствием рост числа ошибок, вызванных внешними помехами. Характерно, что внешние помехи, как правило, вызывают искажение группы смежных бит передаваемого сообщения. Такие групповые

искажения бит сообщения получили название “пачек” ошибок [1].

Вследствие возникновения “пачек” ошибок кратность искаженных битов сообщения значительно превышает число битовых ошибок, вызванных гауссовым шумом или межсимвольной интерференцией. Для коррекции битовых искажений большой кратностей необходимы новые методы и средства контроля ошибок.

Таким образом, проблема повышения эффективности обнаружения и коррекции ошибок, вызванных внешними помехами, в современных условиях является актуальной и имеющей важное практическое значение.

Анализ известных способов коррекции “пачек” ошибок

Доминирующими причинами возникновения ошибок в современных каналах передачи цифровых данных являются межсигнальная интерференция, гауссов шум и внешние помехи [1]. Характер ошибок, обусловленных первыми двумя причинами существенно отличается от тех, которые вызваны внешним шумом. Так, явления межсигнальной интерференции и гауссова шума вызывают независимые искажения отдельных битов информационного, причем зависимость вероятности появления ошибок от их кратности носит биномиальный характер, так, что для описания таких ошибок приме-

нима теоретическая модель двоичного симметричного канала [2].

Для описания ошибок, вызванных внешними помехами используется другая модель [2]. Внешние помехи, как правило, по длительности соответствуют времени передачи группы из h битов. Соответственно, битовые искажения, вызванные внешней помехой ограничены указанной группой битов. Это означает, что искажению могут подвергнуться каждый из h смежных битов сообщения. В дальнейшем, будем считать, что число смежных бит, передаваемых во время действия помехи и, соответственно, подверженных риску искажения не превышает m , то есть $h \leq m$. Таким образом, в рамках рассмотренной модели возникновения ошибок, однократная внешняя помеха может вызвать искажение любого числа из m смежных битов сообщения. При этом группа из m смежных битов сообщения, подверженных искажению под действием внешней помехи получила название “пачки” ошибок [1].

Для обеспечения надежности передачи данных применяется широкий арсенал средств. Однако, развитие технологий передачи цифровой информации имеет следствием постоянное смещение акцентов в оценке эффективности средств обнаружения и коррекции ошибок. Основными критериями средств обеспечения надежности передачи данных являются:

- Надежность контроля ошибок, которая характеризуется классом исправляемых и выявляемых ошибок.
- Надежность классификации класса корректируемых ошибок.
- Временные характеристики: возможность вычисления контрольного кода в темпе передачи данных, время t_1 выявления ошибки, время t_2 коррекции ошибок.
- Число передаваемых контрольных разрядов.

С ростом скорости передачи значимость временных характеристик возрастает, а важность количества передаваемых контрольных разрядов уменьшается.

К настоящему времени для обеспечения надежности передачи цифровых данных применяются две базовые технологии:

- контроль и исправление выявленных ошибок с использованием корректирующих кодов

- выявление ошибок с использованием специальных кодов и исправление ошибок путем повторной передачи информационного блока.

Выбор базовой технологии определяется характеристиками канала передачи данных и особенностями использования. Так, в проводных и кабельных линиях передачи данных интенсивность возникновения ошибок достаточно мала и, поэтому, здесь чаще используется технология обнаружения ошибок с повторной передачей. Напротив, в подверженных внешним помехам беспроводных каналах, в которых интенсивность возникновения ошибок относительно велика, чаще применяют корректирующие коды [3].

При использовании корректирующих кодов их эффективность существенно падает с ростом кратности исправляемых ошибок, поскольку и число необходимых для коррекции контрольных разрядов и вычислительная сложность операций контроля экспоненциально зависят от кратности корректируемых разрядов [3]. При этом корректирующие коды не учитывают особенностей ошибок, возникающих при воздействии внешних помех.

Значительная вычислительная сложность получения синдрома ошибок при их большой кратности создает существенные трудности при реализации контроля в темпе передачи данных для скоростных каналов передачи цифровой информации. Важным недостатком корректирующих кодов является то, что объем вычислений для получения синдрома ошибок постоянен и не зависит от того, произошли они или нет [3]. Вместе с тем, для кабельных линий передачи данных интенсивность возникновения “пачек” ошибок относительно мала и выполнение большого объема вычислений является избыточным.

Существенно меньшее количество контрольных разрядов используется для обнаружения “пачек” ошибок. Наиболее распространенным средством контроля таких ошибок являются циклические избыточные коды (CRC). При использовании CRC “пачка” ошибок гарантированно обнаруживается, если степень n образующего полинома CRC больше или равна длине “пачки” [3]. При этом CRC не гарантирует обнаружения двух и более “пачек” ошибок. Для многих приложений повторная передача блока является

неприемлемой в силу того, что это требует значительного времени и сопряжено с прерыванием потока данных. Такая проблема возникает при передаче данных с использованием кабельных линий в системах реального времени [3].

Таким образом, для достаточно широкого круга приложений, связанных, в первую очередь, с обработкой информации в реальном времени, известные методы не обеспечивают эффективного решения задачи коррекции «пачек» ошибок передачи данных.

Целью исследований является разработка новых, эффективных средств коррекции вызванных внешними помехами «пачек» ошибок в высокоскоростных проводных и кабельных каналах.

Коррекция «пачек» ошибок с использованием взвешенных контрольных сумм

Известно, что наиболее быстрым способом контроля ошибок являются контрольные суммы. Существует ряд их модификаций, наиболее эффективными из которых являются взвешенные контрольные суммы [4]. Важным их достоинством является возможность адаптации к особенностям ошибок доминирующего типа.

Исходя из этого, поставленная цель может быть достигнута путем создания модификации взвешенной контрольной суммы, адаптированной для обнаружения и исправления «пачек» ошибок, вызванных одной или двумя внешними помехами.

Контролируемый блок $B = \{b_1, b_2, \dots, b_n\}$, $\forall l \in \{1, \dots, n\}: b_l \in \{0, 1\}$, логически разделяется на m -битовые символы: $B = \{X_1, X_2, \dots, X_q\}$, $q = n/m$, $\forall j \in \{1, \dots, q\}: X_j = \{b_{(j-1)m+1}, b_{(j-1)m+2}, \dots, b_{jm}\}$. Тогда блок B можно рассматривать как матрицу, строки которой соответствуют символам, а столбцы – одноименным битам символов.

Контрольный код C информационного блока B предлагается формировать в виде $C = \{S_0, S_1, S_2, \dots, S_m, P\}$, где $P = \{p_1, p_2, \dots, p_m\}$ m -битовый вектор, каждый i -тый ($i \in \{1, \dots, m\}$) бит которого равен сумме по модулю 2 i -тых битов всех символов:

$$\forall i \in \{1, \dots, m\}: p_i = x_{1i} \oplus x_{2i} \oplus \dots \oplus x_{qi} = b_i \oplus b_{m+i} \oplus \dots \oplus b_{n-q+i}$$

S_0 – k -битовый ($k = \log_2 q$) код суммы по модулю 2 произведений битов четности символов информационного блока на весовой коэффициент W_j , зависящий от порядкового номера символа в блоке:

$$S_0 = \bigoplus_{j=1}^q W_j \cdot (x_{j1} \oplus x_{j2} \oplus \dots \oplus x_{jm}) \quad (1)$$

В простейшем случае, весовой коэффициент W_j j -го символа совпадает с k -битовым номером этого символа: $W_j = j$. При формировании m -разрядных компонент контрольного кода: S_1, S_2, \dots, S_m используются наборы весовых коэффициентов U_1, U_2, \dots, U_m . Каждый i -тый набор U_i включает в себя q ($k+1$)-разрядных весовых коэффициентов: $U_i = \{u_{i1}, u_{i2}, \dots, u_{iq}\}$, обладающих определенными свойствами. Каждая i -тая компонента S_i контрольного кода C представляет собой ($k+1$)-разрядный код суммы по модулю 2 произведений i -тых битов всех символов блока на соответствующий весовой коэффициент i -то набора U_i

$$\forall i \in \{1, \dots, m\}: S_i = \bigoplus_{j=1}^q u_{ij} \cdot x_{ji} \quad (2)$$

Коэффициенты наборов U_1, U_2, \dots, U_m подбираются таким образом, чтобы выполнялись следующие условия:

1. В рамках одного набора все весовые коэффициенты должны быть отличными друг от друга: $\forall i \in \{1, \dots, m\}, \forall j, e \in \{1, \dots, q\}, j \neq e: u_{ij} \neq u_{ie}$.

2. Для каждой пары U_i и U_v наборов, $\forall i, v \in \{1, \dots, m\}$, сумма по модулю 2 двух любых пар весовых коэффициентов должна быть отличной друг от друга: $\forall j, e, z, y \in \{1, \dots, q\}, j \neq e, j \neq z, e \neq z, e \neq y, z \neq y: (u_{ij} \oplus u_{ie}) + 2^{k+1} \cdot (u_{vj} \oplus u_{ve}) \neq (u_{iz} \oplus u_{iy}) + 2^{k+1} \cdot (u_{vz} \oplus u_{vy})$. Другими словами, недопустимой является совпадение сумм по модулю 2 двух пар весовых коэффициентов для двух наборов.

В таблице 1, в качестве примера, приведены значения наборов U_1, U_2, U_3, U_4 весовых коэффициентов, удовлетворяющие приведенным условиям для $m=4$ и $q=10$.

Из свойства 2 следует, что полученные наборы U_1, U_2, \dots, U_q весовых коэффициентов обеспечивают однозначную локализацию двух символов, в которых искажена одноименная пара бит. В частности, если для приведенных в таблице 1 наборов весовых коэффициентов рассматривать искажения 2-

го и 3-го битов в паре 4-разрядных символов, то для любой пары $r, s \in \{1, \dots, 10\}$ символов пара значений сумм соответствующих коэффициентов $\langle u_{2,r} \oplus u_{2,s}, u_{3,r} \oplus u_{3,s} \rangle$ позволяют однозначно идентифицировать одну из 45 возможных пар $\langle r, s \rangle$. Этот факт иллюстрируется таблицей 2.

Табл. 1. Наборы весовых коэффициентов

Номер символа	Наборы весовых коэффициентов			
	U_1	U_2	U_3	U_4
1	2	2	2	2
2	3	1	1	1
3	4	4	4	4
4	5	3	5	6
5	6	7	3	8
6	7	8	8	3
7	8	5	6	9
8	9	9	11	5
9	10	10	15	10
10	11	14	13	15

Общий объем V_T памяти таблиц соответствия пары сумм весовых коэффициентов паре номеров коэффициентов определяется в виде:

$$V_T = \frac{n \cdot (n - m - q + 1)}{2} \cdot \log_2 q \quad (3)$$

Предлагаемый способ формирования контрольного кода иллюстрируется следующим примером. Пусть передается блок данных, состоящий из 40 бит. Пусть длительность воздействия помехи не превышает времени передачи 4-х символов. Тогда, разрядность m символа принимается равной 4-м. Соответственно блок состоит из 10-ти ($q=10$) 4-х битовых символов: $X_1=\{1001\}$, $X_2=\{0011\}$, $X_3=\{1000\}$, $X_4=\{1111\}$, $X_5=\{1011\}$, $X_6=\{0001\}$, $X_7=\{1100\}$, $X_8=\{0110\}$, $X_9=\{0101\}$, $X_{10}=\{0010\}$. Если при формировании контрольного кода используются наборы весовых коэффициентов U_1, U_2, U_3 и U_4 , приведенные в таблице 1, то компоненты контрольного кода вычисляются в следующем виде: $S_0 = \{1010\}$, $S_1 = \{1101\}$, $S_2 = \{0101\}$, $S_3 = \{0001\}$, $S_4 = \{0100\}$, $P = \{0101\}$.

Табл. 2. Соответствие сумм коэффициентов U_2 и U_3 номерам пары символов, в которых искажены 2-й и 3-й биты.

$u_{2,r} \oplus u_{2,s}, u_{3,r} \oplus u_{3,s}$	r, s	$u_{2,r} \oplus u_{2,s}, u_{3,r} \oplus u_{3,s}$	r, s
1 - 2	3,7	9 - 9	2,6
1 - 3	6,8	9 - 10	4,9
1 - 7	1,4	9 - 14	5,10
2 - 4	2,4	10 - 9	3,10
2 - 5	5,7	10 - 10	1,6
2 - 7	6,9	10 - 14	4,8
3 - 3	1,2	11 - 9	1,8
3 - 4	8,9	11 - 11	7,10
3 - 7	3,5	11 - 13	4,6
4 - 2	9,10	11 - 14	2,9
4 - 6	4,5	12 - 12	3,6
4 - 7	2,7	12 - 13	7,8
5 - 1	1,5	12 - 15	1,10
5 - 5	2,3	13 - 8	4,10
6 - 2	2,5	13 - 12	5,9
6 - 3	4,7	13 - 14	6,7
6 - 5	6,10	13 - 15	3,8
6 - 6	1,3	14 - 8	5,8
7 - 1	3,4	14 - 11	3,9
7 - 4	1,7	15 - 9	7,9
7 - 6	8,10	15 - 11	5,6
8 - 10	2,8	15 - 12	2,10
8 - 13	1,9		

Исправление одной “пачки” ошибок

Если под воздействием внешней помехи возникла “пачка” ошибок, то это означает, что в рамках компактной группы из m битов подверглись искажению от одного до m бит, принадлежащих одному или двум смежным символам. В этой ситуации принципиально исключено искажение двух битов с одинаковыми номерами. Соответственно, ситуация классифицируется путем анализа полей $\Delta S_1, \dots, \Delta S_m$ и ΔP разности контрольных кодов передатчика и приемника: если одноименные коды ΔS и компоненты ΔP оба не равны нулю или оба равны нулю, то считается, что при передаче блока произошла одиночная “пачка” ошибок. Формально: если $\forall g \in \{1, \dots, m\}$ справедливо одно из двух условий: $\Delta S_g \neq 0$ и $\Delta p_g \neq 0$ или $\Delta S_g = 0$ и $\Delta p_g = 0$, то “пачка” ошибок классифицируется как одиночная, искажающая один или пару смежных символов блока.

Если “пачка” ошибок локализована в одном символе, например X_r , где $r \in \{1, \dots, q\}$, то на приемнике будут искажены биты, номера которых принадлежат множеству $\mathcal{Q} \subseteq$

$\{1, 2, \dots, m\}$. Соответственно, биты в коде Δ разности контрольных кодов приемника и передатчика биты Δp поля P равны единице, если их номера принадлежат Θ . Аналогично, коды $\Delta S_1, \Delta S_2, \dots, \Delta S_m$ принимают значение нуля, если их номер не принадлежит Θ и равны r -тому весовому коэффициенту соответствующего набора, если их номера принадлежат Θ : $\forall g \in \Theta: \Delta S_g = u_{gr}$. Код ΔS_0 может быть равным нулю или единице, в зависимости от того четное или нечетное количество элементов содержит множество Θ .

Описанный тип ошибки достаточно просто исправляется: номер r искаженного символа определяет любой ненулевой код $\Delta S_1, \Delta S_2, \dots, \Delta S_m$, а искаженные в этом символе биты выделяют единичные компоненты ΔP .

Если «пачка» ошибок локализована в паре смежных символов, например X_r и X_{r+1} где $r \in \{1, \dots, q\}$, то на приемнике, в символе X_r будут искажены биты, номера которых принадлежат множеству $\Theta \subseteq \{d, \dots, m\}$, а в символе X_{r+1} будут искажены биты, номера которых принадлежат множеству $\Omega \subseteq \{1, \dots, d-1\}$, так, что общее количество искаженных битов в обоих символах не превышает m . Локализация искаженных символов осуществляется следующим образом: ненулевые компоненты $\Delta S_d, \dots, \Delta S_m$ позволяют определить номер r первого из искаженных символов, а ненулевые компоненты $\Delta S_1, \dots, \Delta S_{d-1}$ через соответствующие весовые коэффициенты определяют значение $r+1$. При этом значение d определяется по кодам $\Delta S_1, \Delta S_2, \dots, \Delta S_m$: их ненулевые значения образуют две компактные группы: первая образована весовыми коэффициентами $(r+1)$ -го символа, а вторая – весовыми коэффициентами r -го символа.

Описанная процедура коррекции одной «пачки» ошибок может быть иллюстрирована следующим образом в рамках изложенного выше примера передачи блока из 40 бит.

Пусть под воздействием помехи исказились два смежных символа с номерами 8 и 9, так, что на приемнике получены следующие их значения: $X_8' = \{0111\}$, $X_9' = \{1001\}$. Контрольный код на приемнике вычисляется в следующем виде: $S_0' = \{0010\}$, $S_1' = \{0111\}$, $S_2' = \{1111\}$, $S_3' = \{0001\}$, $S_4' = \{0001\}$, $P' = \{1110\}$. Соответственно, компоненты

разности контрольных кодов приемника и передатчика равны: $\Delta S_0 = \{1000\}$, $\Delta S_1 = \{1010\}$, $\Delta S_2 = \{1010\}$, $\Delta S_3 = \{0000\}$, $\Delta S_4 = \{0101\}$, $\Delta P = \{1101\}$. Поскольку $\Delta p_1 = 1$, то первый бит искажен только в одном символе. Так как $\Delta S_1 = 10$, а в наборе U_1 имеется только один код, равный 10: $u_{19} = 10$, то первый бит искажен в 9-м символе. Аналогично, поскольку $\Delta p_2 = 1$, то второй бит искажен в символе, весовой коэффициент которого в наборе U_2 равен $\Delta S_2 = 10$. Поскольку только $u_{29} = 10$, то второй бит искажен в 9-м символе. Так, как $\Delta p_3 = 0$ и $\Delta S_3 = 0$, то 3-й бит не искажен ни в одном из передаваемых символов. Так как $\Delta p_4 = 1$, то номер символа, в котором искажен 4-й бит находится исходя из значения $\Delta S_4 = 5$. Среди U_5 только $u_{48} = 5 = \Delta S_4$. Следовательно, 4-й бит искажен в 8-м символе.

Таким образом, предложенная модификация взвешенной контрольной суммы позволяет корректировать любые битовые искажения, вызванные однократным воздействием внешней помехи.

Исправление двух «пачек» ошибок

При воздействии двух помех, длительность каждой из которых не превышает времени передачи одного символа, в передаваемом блоке данных может исказиться два, три или четыре символа.

При искажении пары символов, например, r -го X_r и s -го – X_s , $r, s \in \{1, \dots, q\}$ их локализация осуществляется следующим образом. Единичные биты компоненты ΔP разности контрольных кодов приемника и передатчика выделяют биты, которые искажены только в одном из пары символов X_r и X_s . Пусть, например, бит $\Delta p_i = 1$, $i \in \{1, \dots, m\}$. Это означает, что искажению подвергся i -тый бит r -того символа X_r . Численное значение номера r искаженного символа определяется исходя из того, что компонента $\Delta S_i = u_{ir}$, то есть r -тому коду набора U_i весовых коэффициентов. По значению u_{ir} однозначно определяется номер r искаженного символа. В случае, если существует $\Delta p_g = 1$, $g \in \{1, \dots, m\}$ такое, что $\Delta S_g = u_{gs}$, то по описанному выше способу определяется номер s второго из искаженных символов – X_g . Если такого единичного бита ΔP не существует, то находится бит e , $e \in \{1, \dots, m\}$ в котором искажены оба символа X_r и X_g . Этот бит находится исходя

из следующих условий: $\Delta p_e = 0$, $\Delta S_e \neq 0$. Очевидно, что $\Delta S_e = u_{er} \oplus u_{eg}$. Код u_{er} известен, поскольку известны коды e и r . Код весового коэффициента $u_{eg} = \Delta S_e \oplus u_{er}$. По коду u_{eg} находится номер g второго из искаженных символов – X_g .

Наконец, если в обоих символах X_r и X_g искажены одни и те же биты, то все элементы вектора ΔP равны нулю. Пусть пара бит, например, с номерами i и e искажены в обоих символах X_r и X_g . Тогда $\Delta S_i = u_{ir} \oplus u_{ig}$ и $\Delta S_e = u_{er} \oplus u_{eg}$. Согласно свойству 2 весовых коэффициентов пара значений суммы двух элементов наборов U_i и U_e однозначно определяет номера r и g суммируемых элементов этих наборов или, что то же самое, – номера искаженных символов блока. Ясно, что если в обоих символах X_r и X_g искажено более 2-х одноименных бит, то номера символов определяются аналогичным способом. Если в каждом из символов X_r и X_g искажен один и тот же единственный бит, например с номером i , то:

$$\Delta S_0 = r \oplus g, \Delta S_i = u_{ir} \oplus u_{ig} \quad (4)$$

Очевидно, что система линейных уравнений (4) позволяет однозначно определить номера r и g искаженных символов.

Номера искаженных битов в символах X_r и X_g определяются следующим образом. Бит с номером i в символе X_r считается искаженным, если выполняется одно из двух условий: $\Delta p_i = 1$ при $\Delta S_i = u_{ir}$ или $\Delta p_i = 0$ при $\Delta S_i \neq u_{ir}$.

Если две помехи вызвали искажение трех или четырех символов, то при условии, что длительность воздействия одной помехи не превышает времени передачи одного символа, искажению могут быть подвержены не более 2-х одноименных битов в символах.

Пусть, в результате воздействия первой помехи искажены символы X_r и X_{r+1} , а второй – символы X_g и X_{g+1} . При этом, бит с номером i может быть искажен либо в одном из символов X_r или X_{r+1} , и независимо – в одном из символов X_g или X_{g+1} . Если i -тый бит искажен только в символе X_r , то $\Delta p_i = 1$ и $\Delta S_i = u_{ir}$, только в символе X_{r+1} то $\Delta p_i = 1$ и $\Delta S_i = u_{i,r+1}$, только в символе X_g то $\Delta p_i = 1$ и $\Delta S_i = u_{ig}$, только в символе X_{g+1} то $\Delta p_i = 1$ и $\Delta S_i = u_{i,g+1}$. Таким образом, если i -тый бит искажен только в одном символе, локализация

последнего осуществляется достаточно просто.

Если i -тый бит искажен в паре символов, то возможно две ситуации. Первая состоит в том, что существует еще один бит который искажен в паре символов. Вторая ситуация возникает, если не существует другого символа, искаженного в паре символов.

В первой из означенных ситуаций локализация искаженных символов производится следующим образом. Пусть бит с номером i , $i \in \{1, \dots, m\}$ искажен в символе X_r (или X_{r+1}) и символе X_g (или X_{g+1}). Существует также бит с номером e , $e \in \{1, \dots, m\}$, который искажен в символе X_r (или X_{r+1}) и символе X_g (или X_{g+1}). В этом случае $\Delta p_i = 0$, а компонента ΔS_i разности взвешенных контрольных сумм может принимать одно из 4-х значений: $\Delta S_i \in \{u_{ir} \oplus u_{ig}, u_{ir} \oplus u_{i,g+1}, u_{i,r+1} \oplus u_{ig}, u_{i,r+1} \oplus u_{i,g+1}\}$. Аналогично, $\Delta p_e = 0$ и $\Delta S_e \in \{u_{er} \oplus u_{eg}, u_{er} \oplus u_{e,g+1}, u_{e,r+1} \oplus u_{eg}, u_{e,r+1} \oplus u_{e,g+1}\}$. В силу свойства 2 весовых коэффициентов пара значений ΔS_i и ΔS_e однозначно определяет компоненты наборов U_i и U_e , а значит и номера символов, в которых искажены i -тый и e -тый биты.

Таким образом, предложенная модификация взвешенной контрольной суммы гарантирует исправление 2-х, произвольно локализованных в передаваемом блоке “пачек” ошибок, длиной не более m бит.

Оценка эффективности

Основным достоинством предложенной модификации взвешенных контрольных сумм по сравнению с корректирующими кодами является существенно большая производительность, позволяющая контролировать ошибки в темпе передачи данных. При использовании корректирующих кодов контроль ошибок производится путем вычисления синдрома. Вне зависимости от того, произошли ошибки или нет, это время постоянно и равно t_s . При этом код синдрома указывает на локализацию искаженных битов в блоке [3]. Таким образом, при использовании корректирующих кодов объем вычислений, обеспечивающий локализацию возможных ошибок производится всегда, вне зависимости от того, есть они или нет. В силу того, объем вычислений экспоненциально зависит от кратности исправляемых ошибок,

время t_s вычисления синдрома достаточно велико [3].

При использовании разработанной модификации взвешенной контрольной суммы время контроля (обнаружения) – t_r ошибок и время их коррекции – t_k существенно различаются: $t_k \gg t_r$. Фактически, в отличие от корректирующих кодов, вычисление контрольного кода производится посимвольно непосредственно в темпе передачи. При этом несколько символов могут обрабатываться параллельно, так, что темп их обработки определяется задержкой вносимой выполнением логической операции XOR. Это определяет малую временную сложность контроля ошибок в предлагаемой разработке. Вместе с тем, временная сложность исправления ошибок в модификации взвешенной контрольной суммы превышает сложность выполнения аналогичной операции при применении корректирующих кодов: $t_k > t_s$. Однако, для кабельных линий передачи данных интенсивность возникновения ошибок достаточно мала, поэтому необходимость в коррекции ошибок возникает достаточно редко. На практике вероятность корректирования ошибок при передаче блока на 1-2 порядка меньше вероятности того, что блок передан без искажений [3]. С учетом этого, очевидно, что среднее значение временной сложности коррекции ошибок в предложенном варианте взвешенной контрольной суммы существенно меньше, чем при использовании корректирующих кодов. Результаты моделирования показали, что при интенсивности возникновения ошибок 10^{-2} на блок, использование предложенной модификации взвешенной контрольной суммы обеспечивает в 5-8 раз меньшую временную сложность обработки ошибок по сравнению с кодом Рида-Соломона.

По числу передаваемых контрольных разрядов предложенная модификация взвешенной контрольной суммы также эффективнее корректирующих кодов. Это обусловлено тем, что, в отличие от корректирующих кодов, которые допускают произвольную локализацию искаженных битов, взвешенная контрольная сумма ориентирована на то, что искажения имеют вид «пачек», то есть специализирована на частном виде ошибок передачи данных.

Количество h разрядов контрольного кода в предложенной модификации взвешенных контрольных сумм определяется формулой:

$$h = m \cdot (\log_2 q + 3) = m \cdot (\log_2 \frac{n}{m} + 3) \quad (5)$$

При использовании корректирующих кодов, способных исправить все возможные битовые искажения, вызванные 2-мя внешними помехами, или, другими словами, две m -битовые «пачки» ошибок число H контрольных разрядов должно обеспечивать возможность локализации $2 \cdot m$ искаженных битов внутри n -разрядного кода. Поскольку число G возможных размещений $2 \cdot m$ искаженных битов внутри n -разрядного кода определяется формулой:

$$G = \binom{2 \cdot m}{n} = \frac{n!}{(n - 2 \cdot m)! (2 \cdot m)!} \approx n^{2 \cdot m} \quad (6)$$

то число H контрольных разрядов равно:

$$H = \log_2 G \approx 2 \cdot m \cdot \log_2 n \quad (7)$$

Очевидно, что $h < H$. Например, при передаче блока размером в 1 Кбайт ($n=2^{13}$) и если символ равен байту ($m=8$), число разрядов для коррекции 2-х «пачек» битовых ошибок при использовании корректирующих кодов составляет $H=208$, а взвешенной контрольной суммы – $h=106$.

Таким образом, для данного примера, число контрольных разрядов для решения одной и той же задачи контроля ошибок при использовании предложенной модификации взвешенной контрольной суммы в 1.96 раз меньше, чем в корректирующих кодах.

Выводы

В результате проведенных исследований разработан способ коррекции одной или двух «пачек» битовых ошибок в последовательных линиях передачи данных. В основе предложенного способа лежит модификация взвешенной контрольной суммы.

Разработана организация вычисления контрольного кода, классификации и исправления одной и двух «пачек» битовых искажений. Сформулированы требования к выбору весовых коэффициентов для вычисления взвешенных контрольных сумм.

Теоретически и экспериментально показано, что по сравнению с корректирующими кодами реализация предложенного способа имеет меньшую временную сложность, что

позволяет выполнять эффективный контроль ошибок в темпе передачи данных для высокоскоростных каналов передачи данных.

Доказано, что решение задачи коррекции двух “пачек” битовых ошибок достигается в предложенном способе с меньшим числом контрольных разрядов, чем в корректирующих кодах.

Предложенный способ коррекции пачек ошибок на основе взвешенных контрольных сумм может быть эффективно использован для обеспечения надежной передачи цифровых данных в скоростных каналах в условиях помех.

Список литературы

1. Ирвин Дж., Харль Д. Передача данных в сетях: инженерный подход. СПб.: БХВ-Петербург, 2002.- 448 с.
2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. М.: Издательский дом “Вильямс”.- 2004.- 1104 с.
3. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера - 2005.- 319 с.
4. Самофалов К.Г., Марковский А.П., Мулки Яссин Ахмед Ал Бадайнех. Обнаружение и исправление ошибок передачи данных с использованием взвешенных контрольных сумм // Проблеми інформатизації та управління. Збірник наукових праць: Випуск 3(14).-К.,НАУ.- 2008.- С.121-128.

Поступила в редакцию 7.12.2009